Security Policy Derivation

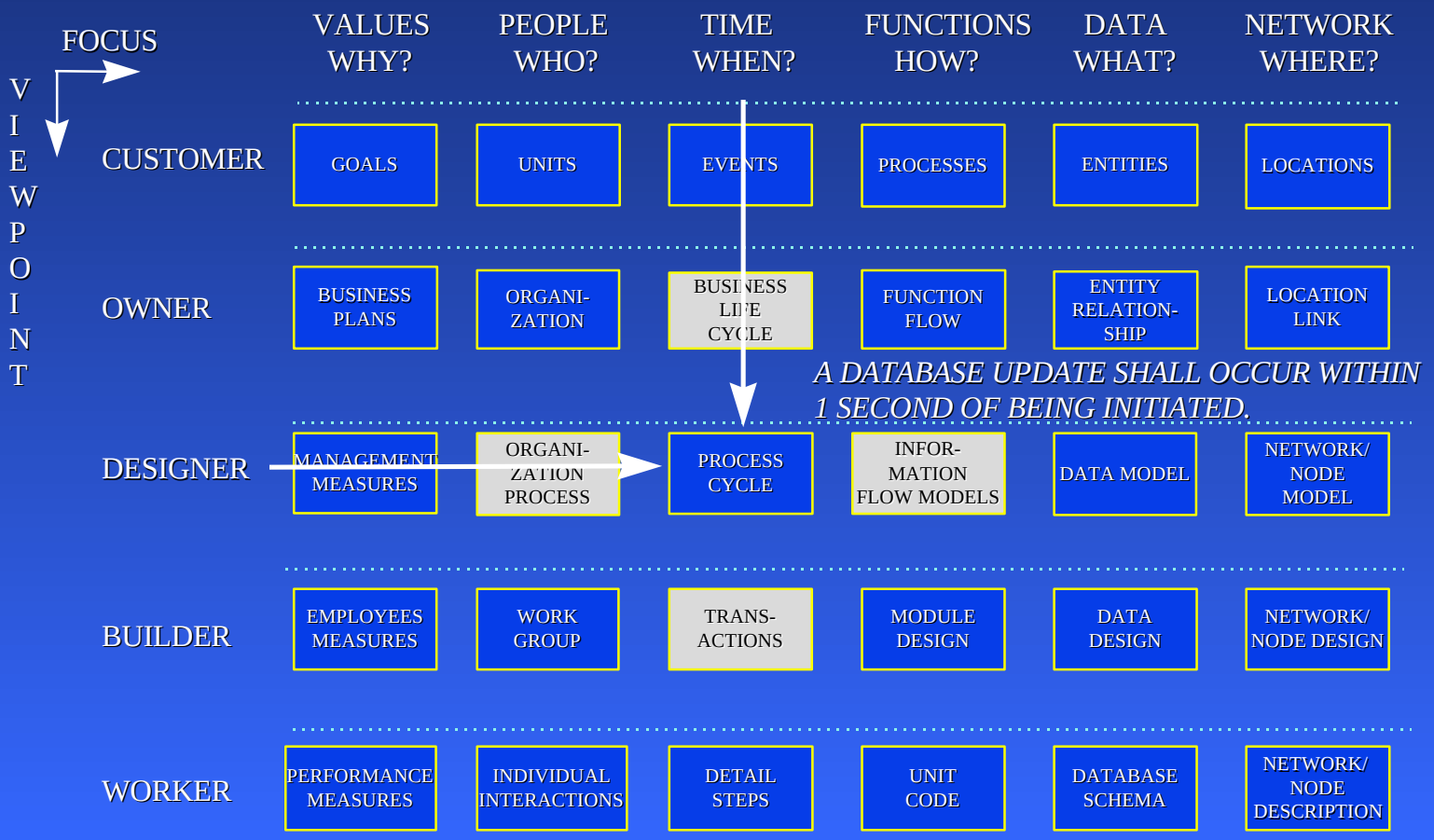
"Thou shalts"
(Directives, ISSO)

"Thou shoulds"
(System Spec)

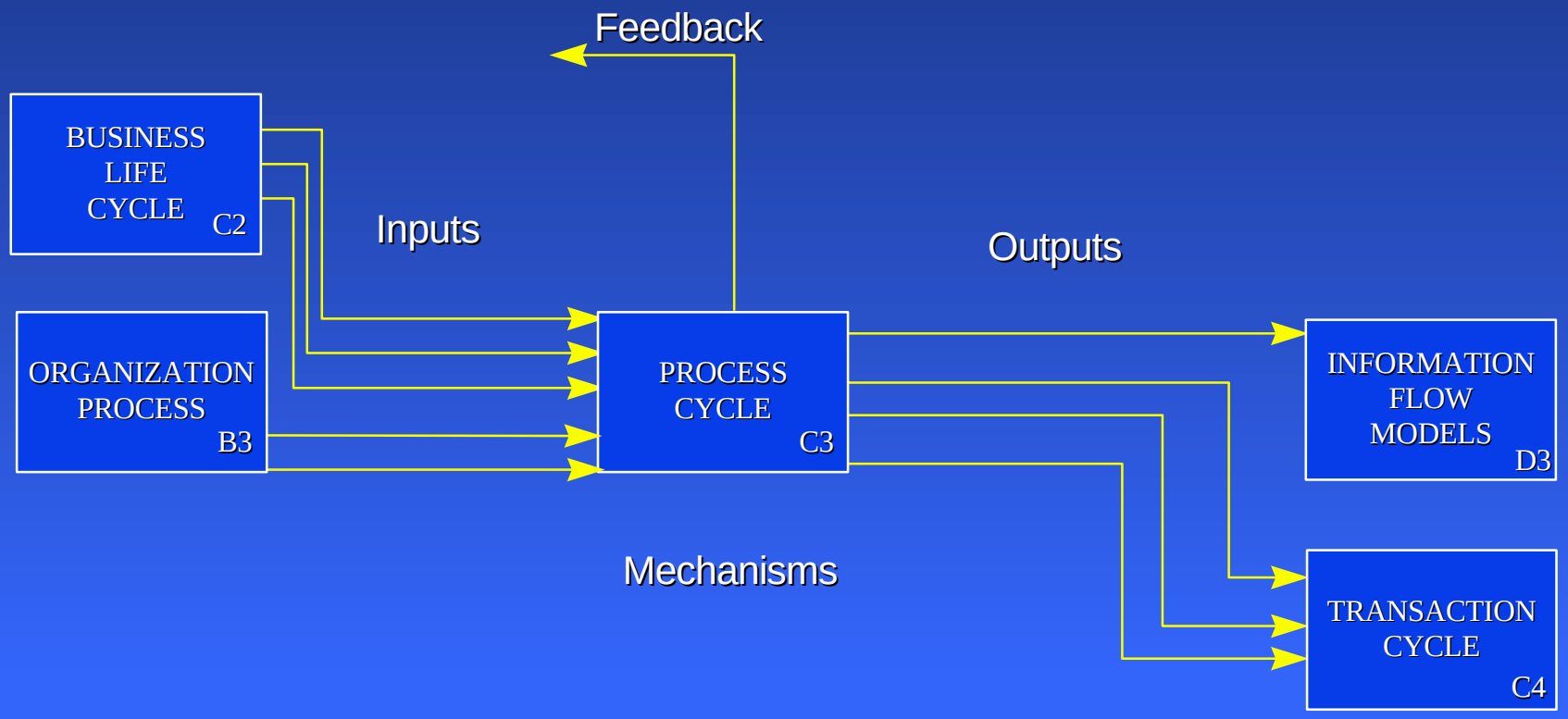
"Thou dids"
(Legacy System)

Actual System Security Policy

The Zachman Framework



IDEF0 Model Cell Example



Security Relevant Information

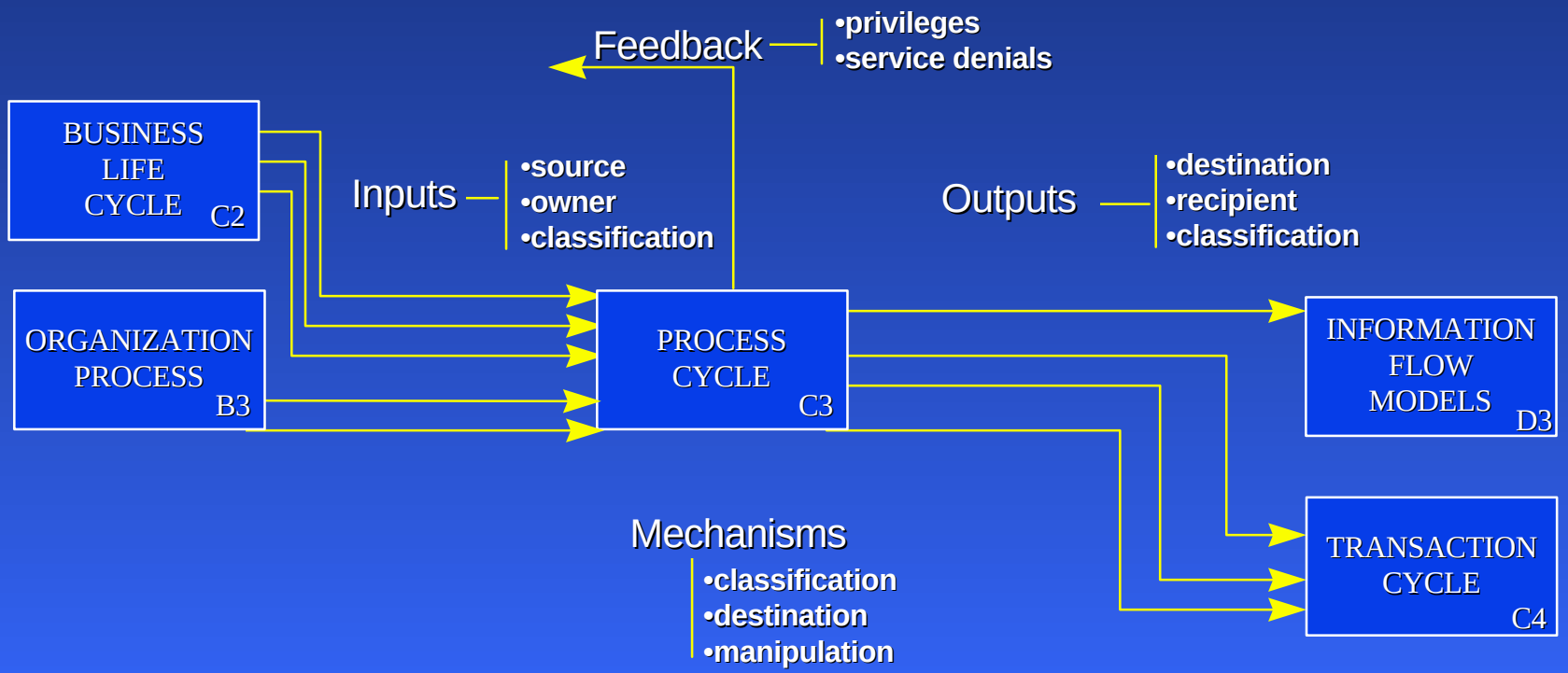
Model Construct

- System Functions
- Information Flows
- Network Connectivity
- Data Model
- "Owners, Modifiers, Users"
- Organization Responsibilities

Security Translation

- What it does
- How Data Moves in the System
- What other systems it talks to
- How Data is Organized
- Who does what to what data
- Who "owns" the data and system processes

IDEF0 Model Cell -- Security Annotated



Security Information -- Annotated

Security Issues

- Classification problems
- User Roles
- Access Control Rules
- Downgrade Policies

Examples

- Mismatched system classification
- Operator, Administrator, User
- User with “X” privilege can do “Y”
- Message release with human in loop only